NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

COURSE 5605

Homeland Defense: Use of the Military Instrument in Strategic Context

Ronald A. Shattuck

FSL: Col. Donn Kegel

Faculty Adviser: Mr. Norm Imler

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2001		**00-00-2001 to 00-00-2001**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Homeland Defense: Use of the Military Instrument in Strategic Context	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National War College,300 5th Avenue,Fort Lesley J. McNair,Washington,DC,20319-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**15**	

Homeland Defense: Use of the Military Instrument in Strategic Context

The 1993 World Trade Center bombing, followed by the sarin gas attack in the Tokyo subway and the tragic events that unfolded at the Oklahoma City Federal Building in 1995, led to a new appreciation of America's vulnerability to terrorist attacks, including attacks that might include the use of chemical or biological agents. Similarly, North Korea's Taepodong missile launch in 1998 led to a reassessment of the threat posed to U.S. territory by rogue states and the need for a National Missile Defense system. In the course of the discussion of the range of actions that the United States would need to take to counter and respond to these threats, the term Homeland Defense came into vogue. The 1997 Quadrennial Defense Review, the report of the National Defense Panel, and the findings of the U.S. Commission on National Security in the 21st Century (Hart-Rudman) all addressed this topic.

There remains, however, a lack of consensus concerning the definition of Homeland Defense, its component elements, and the specific threats that should be subsumed under this concept. Given that the definition of Homeland Defense will impact associated roles, missions, and operational concepts not only of the U.S. Armed Forces, but also of a wide variety of U.S. agencies with responsibilities in the national security area, it is imperative to clarify the terms of reference. Further, to the extent that U.S. armed forces are tasked with a Homeland Defense mission, it should be acknowledged from the outset that there will be significant opportunity costs as limited resources, both budgetary and intellectual, are applied in this area rather than to other missions and priority initiatives.

In this paper the term Homeland Defense (as opposed to alternative formulations such Homeland Security) will be used with the understanding that no a priori assumptions are being made about the use of the military instrument. In fact, it will be argued here that DOD and the U.S. armed forces should only play the lead role in those elements of a Homeland Defense strategy that are well-established as being within the proper domain of the armed forces and where the military instrument can be reasonably expected to make a unique contribution to the achievement of the desired objective. This argument is not based on a strict interpretation of the legal principle of Posse Comitatus, but rather on the belief that U.S. aims can be accomplished most effectively by a coordinated application of the full range of instruments available to policymakers, and that a holistic approach will allow for the integration of diplomatic, law enforcement, and civil libertarian considerations that must be incorporated into a successful approach to the perceived threats. Given the understandable inclination to view the military as a source of ready and effective resources, such an approach will require restraint on the part of policymakers.

A comprehensive and effective Homeland Defense strategy will require a joint approach in the broadest sense of that term: inter-service, interagency, and in conjunction with a range of domestic and international partners. The authors of the CSIS study, "Homeland Defense; A Strategic Approach", have noted that, given the diversity of the threats involved, it would be difficult at best to arrive at a "unified theory of homeland defense".[1] However, as the CSIS report also concluded that, "The U.S. must view homeland defense as a partnership among federal, state, local, and private sector organizations and must fit into U.S. systems of law and concept of federalism." [2]

Development of a Homeland Defense strategy will also have to move beyond discussion of issues related to consequence management and incorporate the concepts of deterrence, prevention, disruption, attribution, and retaliation.

Threats to the Homeland

Bringing clarity to the discussion of Homeland Defense requires focus on the objectives to be achieved, an understanding of the specific threats to the U.S. homeland, and a careful examination of how the available instruments of power might be best used to counter each specific threat. A review of the recent literature suggests that it would be possible to forge a rough consensus that Homeland Defense should be primarily concerned with the dangers posed to the United States by long-range missiles (particularly those systems capable of delivering CBRN to U.S. territory), terrorism (especially those groups that might prove capable of employing CBRN on U.S. territory), and attacks against critical infrastructure that would not only cause significant damage to U.S. economic interests, but might also increase U.S. vulnerability to other forms of attack and loss of life. Each of these threats pose complex conceptual, organizational, and resource problems to policymakers and practitioners engaged in the development of countermeasures. Taken together, the challenge is daunting indeed.

Missiles

In much of the literature on Homeland Defense, emphasis has been placed on the proliferation of long-range missile technology and its accessibility to "rogue states." However, a comprehensive approach to Homeland Defense will necessarily include

consideration of the threat posed by more traditional powers, for example Russia and China, as well. A strategy of deterrence will continue to require the maintenance of U.S. strategic nuclear capabilities, a mission that clearly falls within established DOD responsibilities. Of course, maintenance of these capabilities carries resource implications. At present levels this capability costs approximately 2 percent of the total DOD budget. Whether it will be possible to reduce expenditures further through arms negotiations or even a unilateral reduction of forces remains to be seen. Nonetheless, Stratcom's resource requirements will need to be given due attention for the foreseeable future.

U.S. strategic nuclear capabilities may also serve as a deterrent force against the so-called "rogue states". However, given the less than universal agreement regarding the efficacy of a "traditional" nuclear deterrent strategy against a North Korea or other actors that might threaten the U.S., a case can be made for development and deployment of a National Missile Defense system (NMD) as a key element of the "prevention" component of Homeland Defense. Here again, given that we are talking about a state actor using an offensive military weapon, it is appropriate, per established practice, to assign primary responsibility for this program to DOD. DOD has the established relationships with the private sector contractors and the methodologies in place to develop, test, and procure systems of this nature. And, of course, the Ballistic Missile Defense Office (BMDO) is already fully engaged in this program. Nevertheless, the budget battles and technological issues that are sure to accompany this effort will undoubtedly put a strain on DOD.

The discussion of the missile threat against the U.S. homeland, however, cannot

begin and end with the DOD piece. Neither U.S. nuclear strike capabilities, nor NMD will be sufficient to address all possible missile threats under all potential threat scenarios. Accordingly, deterrence and prevention require active engagement of the Intelligence Community in monitoring threats and tracking proliferation efforts being made by actual and potential adversaries. The diplomatic instrument can also play a critical role through the negotiation of international agreements in the disarmament and counter-proliferation areas. The economic and technological resources available to the U.S. and its allies also should be more aggressively applied in a concerted effort to prevent the proliferation not only of weapons, but also of the expertise required in the development of weapons programs. In other words, greater emphasis and resources should be devoted to programs such as those developed under the Nunn-Lugar Threat Reduction Act.

In the event of a missile attack against U.S. territory, attribution and retaliation requirements will also necessarily involve the Intelligence Community and the Department of State, as well as DOD. These interagency connections, fortunately, are fairly well established. With the approval of the National Command Authorities and similar coordination processes, DOD might also be charged with conducting preemptive or retaliatory strikes using a variety of military capabilities, conventional and strategic. Here the requirements of Homeland Defense do not replace current tasks for the U.S. military, but they are related.

Terrorism

The role of DOD and the U.S. military in countering the threat to the homeland posed by missiles is relatively straightforward and well understood when compared to the level of agreement as to the nature of the threat posed by terrorism and the proper response to that threat. At the outset, it is should be acknowledged that, as noted by Lujan, Posse Comitatus does not pose an insurmountable obstacle to the use of U.S. military assets in support of U.S. law enforcement activities, including counter-terrorism operations.[3] Nonetheless, there are compelling substantive and value-based arguments that support a policy of maintaining distance between military forces and internal security operations. For example, it is clear from the experience of other nations, the British in Ireland for example, that the use of the military in counter-terrorism operations risks conferring a degree of legitimacy on the terrorists as a political actor. Maintaining law enforcement primacy ensures that terrorists and their actions are treated within a criminal context. Handling of terrorists in this manner has proven to be a generally more effective method of preserving popular support for the government's response and counter-measures. This proposal holds true particularly when the government is dealing with a domestic terrorist group rather than a foreign threat.

Along these lines, when military forces are deployed domestically, not only do the issues at hand become more highly politicized, but the risk that excessive force will be utilized also increases dramatically. Military forces act as they have been trained to act – that is to say as soldiers, not as law enforcement officers. Consequently, when it comes to dealing with terrorism, especially terrorist threats on U.S. territory, law enforcement agencies should be given primacy. On the federal level, the FBI should ensure proper

sharing of intelligence information, coordination with local authorities, and the lawful collection of the evidence necessary to proceed with prosecutions in the courts.

Turning specifically to the issue of how best to neutralize foreign terrorist groups that might be willing to take the necessary risks to conduct a successful attack on U.S. territory, deterrence and prevention rely more upon good intelligence, cooperation and coordination with foreign partners, and effective law enforcement than on the direct application of military instrument. As Ambassador Sheehan has argued, the best defense is a good offense conducted abroad.[4] Knowledge of the goals and strategies of each individual group is key to the development of a successful counter-terrorism strategy. Utilization of this intelligence, often in conjunction with foreign partners, can result in the denial of sanctuary to terrorists, restriction of their freedom of movement and access to the resources needed to develop WMD capabilities, and the elimination of terrorist support networks.

Air strikes against terrorist targets, such as at Al-Shiba, can contribute to the effort to deter terrorism. It can also be readily conceded that Special Operations Forces are a counter-terrorism capability that should be retained in the "tool box." However, U.S. intelligence services, law enforcement agencies, and even the Department of State, are better positioned than the military to run the programs needed to address, or at least manage, the terrorism threat at its roots.

As with the missile threat and NMD, since deterrence and prevention efforts abroad cannot absolutely ensure that no adversary will be able to conduct attacks on U.S. territory, attention must be devoted to a second tier of prevention measures. The U.S. border is notoriously porous and there is little question that an effective Homeland

Defense strategy requires that this vulnerability be addressed. However, given the physical characteristics of the border and the strong U.S. interest in the freedom of commerce, it is clear that this will be no easy task. The volume of people, vehicles and cargo that flow across the borders and through U.S. ports of entry provides a favorable environment within which potential terrorists (as well as organized crime and drug-traffickers) can operate.

Here, however, there are non-military options available to enhance the physical security of the homeland, provided adequate resources are made available. The Hart-Rudman commission has proposed the establishment of a National Home Security Agency that would merge the personnel and functions of FEMA, the Coast Guard, The Customs Service, and the Border Patrol. Congressman Mac Thornberry has recently submitted a bill, based upon Hart-Rudman recommendations, that would establish this new agency. Although there is sure to be institutional resistance to the merger, this step would, at a minimum, facilitate the development of shared databases and an improved intelligence product that could be utilized for more effective and efficient interdiction operations at the borders.

No system of border control will prove to be 100 percent effective, but as Ikle has stated, a more robust border control system, i.e. more attention to the prevention piece of the problem, will also force prospective terrorists to undertake higher risk and higher profile entry operations that should prove to be more visible to intelligence collection mechanisms.[5] Along these lines, law enforcement agencies responsible for border control, whether they merge or not, must not only share intelligence obtained from their

own operations, but should also develop stronger links to other sources of information, including Intelligence Community reporting.

Enhancing the capabilities of civilian law enforcement agencies responsible for border control would also have the important, albeit indirect, benefit of significantly diminishing the probability that the military will be implicated in incidents along the border. U.S. forces, such as Task Force 6 at Ft. Bliss, have been deployed along the U.S.-Mexican border in support of law enforcement counter-drug operations. However, the Mexican government has been extremely sensitive to any actions that hint at the militarization of the border. The shooting by a Marine patrol of a 18 year old Mexican American shepherd along the border in 1997 provoked protests not only from the Mexican government, but from civil libertarians in the U.S. as well. Incursions by Mexican military forces across the border as part of the Mexican government's own anti-drug effort, further aggravated the historically strained military to military relationship. The elimination of the military presence on both sides of the border would not only free up military resources for other priority missions, but would eliminate a bone of contention between the U.S. and its neighbor to the south.

The intention here is not to argue that there are no circumstances under which the U.S. military should not assist law enforcement. Rather, the point is that utilization of the military can have unintended consequences and costs. Therefore, it would seem only prudent to fully explore ways to more effectively utilize non-military instruments. It would appear that the DOD leadership under the Clinton administration came to somewhat similar conclusions. Early in the discussion of Homeland Defense, there was consideration with the DOD leadership of creating a CINC for Homeland Defense.

However, in response to the reaction from the American public, a more measured approach to Military Support to Civilian Authorities (MSCA) operations was adopted. Deputy Secretary of Defense Hamre stressed that DOD would never seek any role other than as a supporting force to local law enforcement.[6] Secretary Cohen later acknowledged that DOD had been a bit "premature" in raising the issue of a need for a CINC.[7] The recent creation of a Joint Task Force for Civilian Support in order to facilitate DOD assistance to the consequence management piece of the Homeland Defense problem is, however, wholly consistent with the arguments made here.

Critical Infrastructure

When the discussion turns to protection of critical infrastructure, it becomes even more difficult to achieve the level of clarity that one would desire before attempting to recommend a strategy. However, when critical infrastructure is discussed in the Homeland Defense context the key questions usually boil down to concerns about the physical security of nodes and links (transportation, finance, communication, power) and to the need for Computer Network Defense. Beyond these basic points, however, there is no clear road map regarding roles and missions. Aside from the fact that this issue cuts across internal and interagency organizational lines within the U.S. government, the private sector, which owns and operates most of the nodes and links, is a key factor in this already complicated equation. Since shaping the infrastructure environment needs to be done in peacetime, a working relationship with the private sector must be established and private sector reservations about discussing proprietary information and systems has to be overcome.[8]

The Thornberry Bill, as mentioned above, calls for the creation of a Directorate of Information Operations within the proposed National Homeland Security Agency. This Directorate would absorb the personnel and functions of the FBI's National Information Protection Center and some other existing programs, such as Critical Infrastructure Assurance Office in the Department of Commerce. If the new agency is created, this directorate could serve as the focal point for the development of a core defense capability, an entry point for private sector input, and as a dissemination mechanism for releasable threat information both to private companies and to local authorities. This organizational change would be a good first step and over time perhaps a more effective coordinated and national effort would evolve.

DOD will necessarily retain its own efforts, particularly classified programs, in the Computer Network Attack and Computer Network Defense areas. Nonetheless, DOD can play an especially important role by helping identify critical nodes and links, and by testing systems vulnerabilities. For example, DOD's exercise Eligible Receiver demonstrated the benefits of cooperating with the private sector and the value-added that the USG can bring to the effort to protect private sector, as well as national security, interests.

In short, it will not be easy to develop a solution to the problem of how best to organize an effective defense of America's critical infrastructure. The prevention piece alone will require enhanced vertical coordination between all levels of government and a joint effort horizontally that includes the private sector. Barring a successful, dramatic attack on the infrastructure, this effort will require sustained attention over time. As noted above, the creation of a Directorate of Information Operations would at least give a

home to such a program. The CSIS study recommended that the new administration retain the office of the National Coordinator for Security, Infrastructure Protection and Counter-terrorism within the National Security Council. This suggestion has merit in that continuity in the NSC's engagement in these issues should be maintained to ensure that the new policy team can quickly assess the state of play.

.

Conclusions

This discussion of Homeland Defense was intended to suggest that non-military instruments of power will not only be integral to the execution of a comprehensive strategy, but may also be more effective and appropriate instruments than the military depending upon the nature of the specific threat. Focused tasking and the utilization of all instruments of power, will reduce the opportunity costs and will allow the services and DOD to devote constrained resources (budgetary, manpower, and leadership) to areas where only the military can serve U.S. national security interests.

In the Homeland Defense context, the military clearly must play a leading role in the maintenance of a strategic nuclear deterrent and the development and deployment of a National Missile Defense system. DOD and the armed serves (primarily the National Guard) should also be tasked with a supporting role in consequence management and CND. In order to respond effectively to these requirements, DOD will need to take a fresh look at the organization of the joint staff (especially in the IO area which cuts across the responsibilities of all staffs), and devote sufficient resources to STRATCOM. Providing assistance in the consequence management area will require adequate staffing and budget of JTF for Civil Support and the establishment of a new mission for the

National Guard. This latter requirement will have to be factored into the force structure and war fighting plans. NMD will be a long-term effort requiring senior level attention to the imposing budgetary, technological, and manpower issues that go along with a project of this magnitude.

At the policy level, the NSC will have to play a stronger role ensuring that the contributions made by all federal agencies to the Homeland Defense effort are fully coordinated and maximized. The authors of the CSIS study have recommended that the Vice-President be made responsible for most aspects of Homeland Defense. A National Emergency Planning Council, chaired by the Vice-President, would be formed as a mechanism to bring together the heads of concerned agencies, as well as representatives of the private sector and state governments. This proposal has merit given that unity of effort may require this level of engagement by the administration in order to overcome turf battles and to obtain Congressional support New organizational structures, such as the NHSA should be carefully considered, but it should be recognized that the complexity of the issues involved will resist purely organizational solutions. A sustained and long-term effort across the board will be required to promote the evolution of a truly joint approach to the threats posed to the homeland.

In his comments on Homeland Defense, Ikle has stated that, "…American defense planners need to find a middle ground between wishful neglect and wasteful exaggeration."[9] A holistic approach to Homeland Security will contribute to the effort to find that middle ground.

---

[1] Joseph J. Collins and Michael Horowitz, "Homeland Defense: A Strategic Approach" (Center for Strategic and International Studies, Washington, D.C., December 2000), p. 8

[2] Ibid, p. 7

[3] Thomas R. Lujan, "Legal Aspects of Domestic Employment of the Army", Parameters (Autumn 1997), pp. 82-97
[4] Ambassador Michael A. Sheehan, "The Bestg Homeland Defense is a Good Counterterrorism Offense", Journal of Homeland Defense, (Anser, www.homelanddefense.org), Oct 27, 2000
[5] Fred C. Ikle, "An Argument for Homeland Defense", Washington Quarterly, (Spring 98, vol.21, issue 2), p. 9
[6] William E. Conner, "Deputy Secretary of Defense Dr. John J. Hamre challenges standing committee to lead debate on homeland defense", The Officer (Washington, December 1999)
[7] Elizabeth Becker, "Military Terrorism Operation has a Civilian Focus", New York Times (Jan 9, 2000)
[8] Phil Lacombe and David Keyes, "Defending the American Homeland's Infrastructure", Journal of Homeland Defense (www.homelanddefense.org, Anser, October 27, 2000)
[9]Ikle, p. 9